Abstract

Systems and methods of mitigating attacks, such as Denial of Service (DoS) attacks, in a communications network are presented. Source addresses of packets received at network devices are monitored in relation to known reliable addresses stored in a decision engine. If the source address, as stored in a source table, is known as being legitimate the packets are placed in a high priority queue for transmission at the highest rate. Packets with an unknown address are placed in a lower priority queue, the source address stored in a different source table, and the packet is serviced at a lower rate. Packets that become known to be legitimate are moved from the unknown table to the table from which high priority queues are serviced. In this way, an attacker that employs spoofing techniques is prevented from overtaxing network resources.